SIMPLE UNIVERSAL HASH FOR PLAINTEXT AWARE ENCRYPTION

ABSTRACT OF THE DISCLOSURE

A simple universal hash apparatus and method include input means for inputting at least one of a plurality of Plaintext blocks into an integrity aware encryption scheme using at least one of two secret keys to obtain a plurality of Ciphertext blocks; Plaintext checksum means for computing a Plaintext checksum value from the said plurality of Plaintext blocks; Ciphertext checksum means for processing said plurality of Ciphertext blocks and a third key to obtain a Ciphertext checksum; and combination means for combining the said Plaintext checksum and the said Ciphertext checksum to obtain the simple universal hash value.